

Ben Barnow (*pro hac vice*)
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Telephone: 312.621.2000
Facsimile: 312.641.5504
Email: b.barnow@barnowlaw.com

Richard L. Coffman (*pro hac vice*)
THE COFFMAN LAW FIRM
First City Building
505 Orleans Street, Fifth Floor
Beaumont, TX 77701
Telephone: 409.833.7700
Facsimile: 866.835.8250
Email: rcoffman@coffmanlawfirm.com

Interim Co-Lead Counsel

Jeremiah Frei-Pearson (*pro hac vice*)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
1311 Mamaroneck Avenue, Suite 220
White Plains, NY 10605
Telephone: 914.298.3281
Facsimile: 914.824.1561
Email: jfrei-pearson@fbfglaw.com

Marc L. Godino (*pro hac vice*)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310.201.9150
Facsimile: 310.201.9160
Email: mgodino@glancylaw.com

Interim Co-Lead Counsel

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

IN RE:

**ZAPPOS.COM, INC. CUSTOMER DATA
SECURITY BREACH LITIGATION**

This Document Relates To:

All Cases

**Case No. 3:12-cv-00325-RCJ-VPC
MDL No. 2357**

**PLAINTIFFS' THIRD AMENDED
CONSOLIDATED CLASS ACTION
COMPLAINT**

Plaintiffs Theresa D. Stevens, Stacy Penson, Tara J. Elliot, Brooke C. Brown, Christa Seal, Denise Relethford, Emily E. Braxton, Stephanie Preira, Robert Ree, Patti Hasner, Dahlia Habashy, Zetha Nobles, Kristin O'Brien, and Terri Wadsworth (collectively, "Plaintiffs"), on behalf of themselves and all other persons similarly situated, file this Third Amended

Consolidated Class Action Complaint (“CAC”) against Defendant Zappos.com, Inc. (“Zappos” or “Defendant”), and respectfully allege the following:

NATURE OF THE ACTION

1. Plaintiffs, individually and on behalf of over 24 million similarly situated persons (the “Class Members”), bring this consumer class action seeking redress for Zappos’ intentional, willful, reckless, or negligent violations of their privacy rights.
2. Plaintiffs and Class Members are consumers who purchased shoes, apparel, and other merchandise from Zappos, an online retailer and wholly-owned subsidiary of Amazon.com. As part and parcel of their purchase transactions, Plaintiffs and Class Members (i) entrusted their confidential personal customer account information including, *inter alia*, their names, email addresses, billing and shipping addresses, phone numbers, and credit and debit cards to Zappos, and (ii) created a Zappos.com website account password (collectively, “personally identifiable information” or “PII”) (see below). Zappos betrayed Plaintiffs’ and Class Members’ trust by failing to properly safeguard and protect their PII in violation of various states’ statutes and common law.
3. Sometime prior to January 16, 2012, certain of Zappos’ unprotected computer system servers were targeted by fraudsters, breached by the fraudsters, and improperly disclosed Plaintiffs’ and Class Members’ PII to the fraudsters without authorization (the “Data Breach”).
4. During the early morning hours of January 16, 2012, Zappos sent Plaintiffs and Class Members a scant 24-line email notifying them that its servers had been breached and their PII wrongfully disclosed and compromised. Knowing its telephone system was inadequate to handle the onslaught of expected calls reporting identity theft and identity fraud, Zappos also closed its customer service telephone lines for the week immediately

following the Data Breach, requiring its customers to submit their complaints via email. They did, by the scores; their emails provide a written record of the damage wreaked by the Data Breach.

5. Zappos flagrantly disregarded Plaintiffs' and Class Members' privacy rights by intentionally, willfully, recklessly, or negligently failing to take the necessary precautions required to safeguard and protect their PII from unauthorized disclosure. Plaintiffs' and Class Members' PII was improperly handled and stored, and either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols. Zappos' intentional, willful, reckless, or negligent disregard of Plaintiffs' and Class Members' privacy rights caused one of the largest unauthorized disclosures of PII in history.

6. *After* the Data Breach, Zappos immediately took "substantial steps to protect its customers' [PII] from improper access" that it should have taken *before* the Data Breach, including [REDACTED]

[REDACTED]
[REDACTED] But this is the equivalent of locking the barn door after the horse got out.

7. Plaintiffs have standing to bring this suit because as a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) economic damages, and other actual injury and harm, in the form of (i) actual identity theft or identity fraud, (ii) the untimely and/or inadequate notification of the Data Breach, (iii) unauthorized disclosure of their PII, (iv) loss of customer service access that was part of the services provided for by Zappos, including closure of Zappos' customer service telephone lines, which Zappos willfully severed at a time of high need by its customers, (v) loss of the unencumbered use of their extant passwords and the loss of their passwords, (vi) the oppressive Zappos.com website arbitration clause and Zappos' attempted enforcement of same, (vii) invasion of privacy, (viii) breach of the confidentiality of their PII, (ix) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud¹ pressed upon them by the Data Breach, (x) the value of their time spent mitigating the impact of the Data Breach and mitigating increased risk of identity theft and/or identity fraud including, *inter alia*, changing their Zappos.com account passwords and passwords for other accounts using the same passwords, (xi) deprivation of the value of their PII, for which there is a well-established national and international market, (xii) receipt of a diminished value

¹ According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

of the services they paid Zappos to provide (e.g., protection of their PII), (xiii) the impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm, and (xiv) damages incurred by Zappos' violation of the contractual agreement to settle this case—for which they are entitled to compensation.

8. Zappos' wrongful actions, inaction, omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII constitute (i) violations of various state deceptive trade practices, consumer protection, and data breach notification statutes, (ii) negligence/gross negligence, and (iii) unjust enrichment/assumpsit.

9. Plaintiffs, on behalf of themselves and Class Members, seek actual damages, consequential damages, nominal damages, exemplary damages, double or treble damages (as available), injunctive relief, attorneys' fees, litigation expenses, and costs of suit.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Plaintiffs' claims pursuant to 28 U.S.C. § 1332(d) (CAFA) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Zappos' citizenship, and (c) the matter in controversy exceeds \$5 million, exclusive of interest and costs. This Court also has subject matter jurisdiction over Plaintiffs' claims pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over Zappos because at all relevant times, Zappos conducted (and continues to conduct) substantial business in the District of Nevada.

12. Venue is appropriate in this Court pursuant to 28 U.S.C. § 1391 because (i) Zappos is subject to personal jurisdiction in the District of Nevada, (ii) per Zappos, the unauthorized release and disclosure of Plaintiffs' and Class Members' PII giving rise to their claims was made through Zappos' servers located in Nevada, and (iii) at all relevant times,

Zappos resided, was located, was found, conducted substantial business in the District of Nevada (and continues to do so).

13. The class action lawsuits included in this CAC were transferred to this Court and consolidated for pre-trial proceedings by order of the Judicial Panel on Multi-District Litigation. Plaintiffs, however, reserve their right to remand these actions to the districts from which they were transferred at, or before conclusion of, the pre-trial proceedings. *See Lexecon, Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26 (1998).

PARTIES

14. Plaintiff Theresa D. Stevens (“Stevens”) is a resident of Texas. Zappos possesses Stevens’ PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Stevens supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Stevens received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Stevens has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

15. To mitigate the damage caused by the Data Breach, Stevens spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Stevens also has suffered (and will

continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. *See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009)* (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

16. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Stevens’ PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Stevens would choose the latter. Stevens—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Stevens’ PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

17. Plaintiff Stacy Penson (“Penson”) is a resident of Florida. Zappos possesses Penson’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Penson supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Penson received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of

the Data Breach. Penson has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

18. To mitigate the damage caused by the Data Breach, Penson spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Penson also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Penson's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Penson would choose the latter. Penson—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Penson's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

19. Plaintiff Tara J. Elliott (“Elliott”) is a resident of Alabama. Zappos possesses Elliott’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Elliott supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Elliott received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Elliott has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

20. To mitigate the damage caused by the Data Breach, Elliott spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Elliott also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Elliott’s PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and

otherwise used without her authorization versus selling her PII and receiving the compensation herself, Elliott would choose the latter. Elliott—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Elliott’s PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

21. Plaintiff Brooke C. Brown (“Brown”) is a resident of Alabama. Zappos possesses Brown’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Brown supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Brown received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Brown has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

22. To mitigate the damage caused by the Data Breach, Brown spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Brown also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right.

Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Brown's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Brown would choose the latter. Brown—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Brown's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

23. Plaintiff Christa Seal ("Seal") is a resident of Alabama. Zappos possesses Seal's PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos' website, when Seal supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Seal received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Seal has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

24. To mitigate the damage caused by the Data Breach, Seal spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate

result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Seal also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Seal's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Seal would choose the latter. Seal—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Seal's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

25. Plaintiff Denise Relethford (“Relethford”) is a resident of California. Zappos possesses Relethford’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Relethford supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Relethford received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Relethford has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a

regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

26. To mitigate the damage caused by the Data Breach, Relethford spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Relethford also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Relethford’s PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Relethford would choose the latter. Relethford—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Relethford’s PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

27. Plaintiff Emily E. Braxton (“Braxton”) is a resident of Florida. Zappos possesses Braxton’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Braxton supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Braxton received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Braxton has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

28. To mitigate the damage caused by the Data Breach, Braxton spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Braxton also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Braxton’s PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her

PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Braxton would choose the latter. Braxton—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Braxton’s PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

29. Plaintiff Stephanie Preira (“Preira”) is a resident of New York. Zappos possesses Preira’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when Preira supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Preira received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. She meticulously protects her PII.

30. To mitigate the damage caused by the Data Breach, Preira spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Preira also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Preira’s PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not

already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Preira would choose the latter. Preira—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Preira’s PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

31. Plaintiff Robert Ree (“Ree”) is a resident of California. Zappos possesses Ree’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on his review of Zappos’ website, when Ree supplied his PII to Zappos, he believed Zappos would safeguard and protect it. On January 16, 2012, Ree received an email from Zappos notifying him that his PII had been disclosed, without authorization, and compromised as part of the Data Breach. Ree has never been victimized by a data breach other than the Zappos Data Breach. He meticulously protects his PII.

32. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Ree also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of his PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Ree’s PII is now available on the open market, he would receive far less for it now if he attempted to sell his PII—which he is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced

with the choice of having his PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without his authorization versus selling his PII and receiving the compensation himself, Ree would choose the latter. Ree—not fraudsters—should have the exclusive right to monetize his PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Ree's PII also placed him at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

33. Plaintiff Patti Hasner ("Hasner") is a resident of Florida. Zappos possesses Hasner's PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos' website, when Hasner supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Hasner received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Hasner meticulously protects her PII.

34. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, in late January 2012, Hasner's AOL email account, which had the same username and password as her Zappos.com account, was accessed by hackers and used to send unwanted advertisements to people in her address book. To mitigate the damage caused by the Data Breach, Hasner spent time changing the passwords on her AOL account and bank account—at the strong recommendation of Zappos in its Data Breach notification email—and dealing with the consequences of unsolicited mail sent from her AOL account. She also purchased a credit and personal identity monitoring service to alert her to the potential misappropriation of her identity to combat any further identity theft or identity fraud.

35. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Hasner also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Hasner's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Hasner would choose the latter. Hasner—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Hasner's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

36. Plaintiff Dahlia Habashy (“Habashy”) was a resident of Massachusetts at the time of the Data Breach. Zappos possesses Habashy's PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos' website, when Habashy supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, when Habashy was a resident of Massachusetts, she received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach.

37. To mitigate the damage caused by the Data Breach, Habashy spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email. She also purchased a credit and personal identity monitoring service to alert her to the potential misappropriation of her identity to combat any further identity theft or identity fraud.

38. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Habashy also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Habashy's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the compensation herself, Habashy would choose the latter. Habashy—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Habashy's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

39. Plaintiff Zetha Nobles (“Nobles”) is a resident of California. Zappos possesses Nobles' PII, which Zappos was (and continues to be) required to safeguard and protect. Based on

her review of Zappos' website, when Nobles supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, Nobles received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach.

40. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, in January 2012, Nobles' AOL email account, which had the same username and password as her Zappos.com account, was accessed by hackers and used to send unwanted advertisements to people in her address book. To mitigate the damage caused by the Data Breach, Nobles spent time changing the passwords on her Zappos.com account, AOL account, and bank accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email.

41. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, Nobles also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Nobles' PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus

selling her PII and receiving the compensation herself, Nobles would choose the latter. Nobles—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos’ wrongful and unauthorized disclosure of Nobles’ PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

42. Plaintiff Kristin O’Brien (“O’Brien”) is a resident of New York. Zappos possesses O’Brien’s PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos’ website, when O’Brien supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, O’Brien received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. O’Brien has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements. To mitigate the damage caused by the Data Breach, O’Brien spent time changing the password on her Zappos.com account and other accounts using the same password—at the strong recommendation of Zappos in its Data Breach notification email.

43. As a direct and proximate result of Zappos’ wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, on January 25, 2012, O’Brien, an NYPD officer, received a “welcome letter” from Sprint thanking her for opening an account with two telephone lines and purchasing multiple telephones—none of which she did. The next day, she received a similar letter from AT&T regarding the purchase

of three telephones she did not purchase. O'Brien spent a considerable amount of time (approximately two hours a day for a week and a half) on the telephone with Sprint and AT&T closing these accounts and extinguishing the account balances, including multiple telephone calls with an attorney to whom Sprint and AT&T had turned over the accounts for collection. Fraudsters also opened a Radio Shack in-store credit account in her name to which they charged over \$400 of merchandise. Additional fraudulent purchases were made at Radio Shack using O'Brien's compromised Chase Visa credit card tied to her Zappos.com account.

44. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of her PII, and the above-described identity theft and identity fraud, O'Brien locked and unlocked her credit reports, incurring \$30 of fees. On an annual basis at the cost of \$125 per year for 2012-2015, she also purchased credit monitoring to combat future identity theft/identity fraud

45. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, O'Brien also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since O'Brien's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus

selling her PII and receiving the compensation herself, O'Brien would choose the latter. O'Brien—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of O'Brien's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

46. Consistent with the experiences of other Class Members (see table below), Zappos falsely represented to O'Brien over the telephone (once she got through) that Zappos was not responsible for the Data Breach, her Chase Visa credit card was not taken in the Data Breach, and the Data Breach was not the cause of the fraudulent charges on the card and the identity theft and identity fraud she had experienced. Zappos' customer service representative denied her request for credit monitoring, was unhelpful, and generally treated her shabbily.

47. Plaintiff Terri Wadsworth ("Wadsworth") is a resident of Louisiana. Zappos possesses Wadsworth's PII, which Zappos was (and continues to be) required to safeguard and protect. Based on her review of Zappos' website, when Wadsworth supplied her PII to Zappos, she believed Zappos would safeguard and protect it. On January 16, 2012, while living in Michigan, Wadsworth received an email from Zappos notifying her that her PII had been disclosed, without authorization, and compromised as part of the Data Breach. Wadsworth has never been victimized by a data breach other than the Zappos Data Breach. She meticulously protects her PII. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She regularly shreds her hard copy credit card and financial account statements.

48. Up until the Data Breach, Wadsworth was a substantial seller on Ebay, attaining a 1300 Five Star seller rating that took ten years to achieve. In order to achieve this rating, she was required to be in good standing with PayPal. Wadsworth used the same user name and password on her Zappos.com and Ebay accounts. The same email address and debit card was tied to both accounts. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, the fraudsters used her debit card to overdraw her bank account, which the bank unilaterally closed. The fraudsters also hacked her Paypal account, generating a \$1000 balance that Paypal requires Wadsworth to pay in order to continue selling on Ebay. Until the balance is paid, her selling business, and corresponding revenue stream, are shut down—which is a catch-22 because she cannot pay the balance the fraudsters ran-up on Paypal without her Ebay income.

49. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of her PII, and in addition to the above-described damages, Wadsworth also has suffered (and will continue to suffer) economic damages and other actual injury and harm (as detailed above), including, without limitation, the deprivation of the full value of her PII, for which there are well-established national and international markets. PII is a unique and valuable property right. Moreover, once PII is out, it is gone. The fundamental economic principle of supply and demand supports the fact that since Wadsworth's PII is now available on the open market, she would receive far less for it now if she attempted to sell her PII—which she is able to do—than had the PII not already been wrongfully released and disclosed by Zappos. Faced with the choice of having her PII wrongfully released, disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without her authorization versus selling her PII and receiving the

compensation herself, Wadsworth would choose the latter. Wadsworth—not fraudsters—should have the exclusive right to monetize her PII at the highest possible value. Zappos' wrongful and unauthorized disclosure of Wadsworth's PII also placed her at an impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm.

50. Defendant Zappos.com, Inc. is a Delaware corporation with its principal place of business in Las Vegas, Nevada. Zappos is an online retailer of apparel, shoes, handbags, home furnishings, beauty products, and accessories through its websites, Zappos.com and 6pm.com. Zappos has annual sales of over a \$1 billion USD. At all relevant times, Zappos sold apparel, shoes, handbags, home furnishings, beauty products, and accessories to Plaintiffs and Class Members in retail consumer transactions—to wit, in order to receive such merchandise from Zappos, they were required to provide Zappos with their PII and create a Zappos.com account password. At all relevant times, Zappos was (and continues to be) entrusted with, and obligated to safeguard and protect, Plaintiffs' and Class Members' PII. Zappos is a wholly-owned subsidiary of Amazon.com, Inc., the world's largest online retailer with 2014 revenue of over \$88 billion USD. Zappos already has been served with Summons and appeared in this litigation.

FACTS

I. Personally Identifiable Information (PII).

51. Personally identifiable information" or "PII" is information that can be used to *distinguish* or *trace* an individual's identity, such as their name, Social Security number, and biometric records, alone, or when combined with other personal or identifying information that is *linked* or linkable to an individual, such as their birthdate, birthplace, and mother's maiden name. *See, e.g.,* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16; NAT'L INST. OF

STANDARDS & TECHNOLOGY, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), NIST SPECIAL PUBLICATION 800-122 (April 2010), at 2-1 (emphasis added). PII includes, without limitation:

- Name, maiden name, mother's maiden name, or alias;
- Personal identification numbers, such as a Social Security number, passport number, driver's license number, taxpayer identification number, financial account numbers, credit card and debit card numbers, PIN numbers;
- Passwords and user names for financial accounts, payment card accounts, transactional accounts, retail accounts, and other online accounts;
- Address information, such as street addresses, email addresses, and IP addresses;
- Personal characteristics, including photographic images (especially of face or other distinguishing characteristic), fingerprints, handwriting, or other biometric images or template data (e.g., retina scans, voice signature, facial geometry);
- Telephone numbers;
- Vehicle registration plate numbers; and
- Information about an individual that is linked or linkable to one of the above (e.g., birthdate, birthplace, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, and financial information).

52. To *distinguish* an individual is to identify an individual. GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), at 2-1.

53. To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. *Id.* For example, an audit log containing records of user actions could be used to trace an individual's activities.

54. *Linked* information is information about, or related to, an individual that is logically associated with other information about the individual. *Id.* In contrast, "linkable information" is information about, or related to, an individual for which there is a possibility of

logical association with other information. For example, if two databases contain different PII elements, a fraudster with access to both databases may be able to link the information from the two databases and identify an individual, as well as access additional information about or relating to the individual. If the secondary information source is present on the same system or a closely-related system, and does not have security controls that effectively segregate the information sources, the data is linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (*e.g.*, via an internet search engine), the data is linkable.

55. PII does not include only data that can be used to directly identify or contact an individual (*e.g.*, name, e-mail address), or personal data that is especially sensitive (*e.g.*, Social Security number, bank account number, payment card numbers). The OMB and NIST definition of PII is broader. The definition is also dynamic, and can depend on context. Data elements that may not identify an individual directly (*e.g.*, age, height, birthdate, account passwords) nonetheless constitute PII when—such as here—these data elements can be combined, with or without additional data, to identify an individual. In other words, if the data is linked or linkable to a specific individual, it is PII.

56. Moreover, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the “mosaic effect.”

FEDERAL CHIEF INFORMATION OFFICERS COUNCIL, RECOMMENDATIONS FOR STANDARDIZED IMPLEMENTATION OF DIGITAL PRIVACY CONTROLS (Dec. 2012), at 7-8.

II. The Zappos Data Breach.

57. On Zappos' online retail websites, Zappos.com and 6pm.com, Zappos' customers create accounts to purchase shoes, apparel and other merchandise. The customer accounts contain PII—which includes, *inter alia*, their names, account numbers, passwords, e-mail addresses, billing and shipping addresses, telephone numbers, and the last four digits of their credit cards and debit cards. Each account is accessed by the customer using a unique username and password.

58. At all relevant times, in the “Privacy Policy” on its website, Zappos represented that “[a]ccess to your personal information is restricted. Only employees who need access to your personal information to perform a specific job are granted access to your personal information.” Zappos also represented that it “take[s] several steps to protect your personal information in our facilities.”

59. Zappos also made a “Safe Shopping Guarantee,” promising that the use of credit card information on its websites is secure.

60. Zappos also placed a yellow, lock-shaped icon on its website payment page that confirmed entry of a consumer’s PII as part of an online retail transaction with Zappos was “safe and secure.”

61. Zappos, however, did not live up to its “Privacy Policy,” “Safe Shopping Guarantee,” and other promises and representations regarding the safety and security of Plaintiffs’ and Class Members’ PII. As evidenced by the above-described belated Data Breach data security measures it immediately implemented, Zappos failed to properly safeguard and protect Plaintiffs’ and Class Members’ PII, thereby resulting in the Data Breach and its wrongful and unauthorized disclosure.

62. On January 16, 2012, in the middle of the night, Plaintiffs and over 24 million Class Members received a scant 24-line, carefully crafted, less-than-forthcoming email from Zappos notifying them that certain parts of their PII had been disclosed to fraudsters and compromised:

We are writing to let you know that there may have been illegal and unauthorized access to some of your customer account information on Zappos.com, including one or more of the following: your name, e-mail address, billing and shipping addresses, phone number, the last four digits of your credit card number (the standard information you find on receipts), and/or your cryptographically scrambled password (but not your actual password).

What the email does not say is as powerful as what it does—while the Data Breach included the above-listed categories of PII, it was not limited to the above-listed categories of PII. This, in fact, turned out to be the case as demonstrated by the customer communications summarized in the table below. Zappos' representation in the email that “[t]he database that stores your critical credit card and other payment data was NOT affected or accessed” was false. It was.

63. According to Tony Hsieh, Zappos' CEO, Plaintiffs' and Class Members' PII was obtained by hackers who targeted weaknesses in Zappos' internal computer system, gaining access to the computer system via unprotected servers.

64. As a direct and proximate result of Zappos' failure to safeguard and protect Plaintiffs' and Class Members' PII including, *inter alia*, failing to maintain a proper firewall, failing to properly encrypt the PII, failing to implement the above-described data security policies, procedures, and protocols (which Zappos implemented immediately *after* the Data Breach), and violating standard industry data security practices and procedures,² Plaintiffs' and

² The FTC suggests that businesses adhere to certain guidelines to protect against the unauthorized disclosure of PII in their files, including:

Class Members' PII was disclosed and compromised, and their privacy invaded. The compromised PII was private, confidential, and sensitive and, on information and belief, unencrypted or improperly encrypted in Zappos' internal computer system.

65. Further compounding the problem, Zappos closed its customer service telephone lines after the Data Breach was announced which, in turn, prevented Plaintiffs and Class Members from contacting Zappos about the Data Breach, discussing the details of the Data Breach with a human being, and learning about the nature and extent of their compromised PII which, in turn, delayed implementation of appropriate and reasonable security measures to prevent identity theft and identity fraud. The Plaintiffs' above-described post-Data Breach experiences provide examples of the actual confusion, injury and harm suffered by Plaintiffs because of Zappos' unilateral closure of its (admittedly inadequate) customer service telephone lines in the face of a data breach crisis.

- a. Do not collect confidential PII if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;
- b. Encrypt the confidential PII—particularly if it is shipped to outside carriers or contractors;
- c. Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;
- d. Control access to sensitive PII requiring that employees use “strong” passwords; tech security experts believe the longer the password, the better; and
- e. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to PII.

See FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. Zappos also failed to follow the guidelines suggested by the FTC in this publication by its unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

66. Fortunately, Zappos at least entertained customer emails inquiring about the Data Breach, reporting its impact, and asking whether Zappos intended to compensate them or provide post-Data Breach data security protection, such as credit monitoring. Like broken records, Zappos' customer service representatives, working from carefully scripted talking points, repeated the corporate mantra in emails to, and telephone conversations with, Plaintiffs and Class Members, their customers; to wit, Zappos falsely and uniformly represented to Plaintiffs and Class Members that it was not responsible for the Data Breach, their credit card and debit card numbers were not taken in the Data Breach, and the Data Breach was not the cause of their subsequent fraudulent charges, identity theft/identity fraud, and other post-Data Breach experiences—which, as demonstrated above and below, were false statements.

67. The limited number of unredacted³ customer emails, call-in records (after the telephone lines were re-opened), and fraudulent transaction chargebacks evidencing post-Data Breach identity theft and identity fraud that Zappos has produced to date are summarized below:

DATE	ZAPPOS DOC. NO.	CUSTOMER COMPLAINTS
1/13/2012	ZAP0011925	"I never placed this order with you. Please cancel it. My account was stolen by the hacker I think. I already changed the password for this account."
1/16/2012	ZAP0003376	[Customer email]. "I am assuming that you know about the VIP.Vappos.com site. While I was trying to change my password this evening I stumbled into this site and got out of it without doing a lot of damage."
1/16/2012	ZAP0003380-81	[Customer email]. "I received your email with instructions on changing my password. However, I was directed to call an 800 number and when answered, a customer service rep told me that due to your problems I was entitled to a \$100 gift certificate! He then asked for my mailing address and my email address which I gave him as I knew they had been 'hacked' and were not invasive. When he asked for a credit card number to pay for

³ A substantial amount of the post-Data Breach customer emails, call-in records, and fraudulent transaction chargeback records produced by Zappos to date are completely redacted, black pages.

		the \$3.95 charge to receive my \$100 gift certificate, I refused to do so emphatically and requested to speak with his supervisor. I was told he had to have the credit number before he could transfer my call! I IMMEDIATELY DISCONNECTED THE CALL!!!"
1/16/2012	ZAP0003385-86	[Customer email]. "Hi, I received the email about the security breach and manually entered "zappos.com" in the browser address line to go to your site and reset my password. I got a popup window saying I was the daily gift card winner for the San Francisco area -- for a \$500 Zappos gift card. The form asked for my name, mobile phone #, and email address, and displays the gift card # and PIN#. Here's the URL: http://c53905.info/859e1ea74dc6/ I'm not filling out the form until I know if this is for real. Did I really win a Zappos gift card or is this part of the security breach?"
1/16/2012	ZAP0003402	[Customer email]. "Are you nuts? Do you think that this email makes it okay? Do you think we don't even deserve an apology? I haven't even visited your website since 2007, so you should have deleted my account a long time ago. A few weeks ago I began receiving strange emails directed as someone else. I realize now this is probably your fault."
1/17/2012	ZAP0003406	[Customer email]. "I received a phone call today claiming that I placed an order, but the credit card didn't go through, wanted me to call and give my credit card number. The truth is that I did not place any order lately, I suspect this has something to do with your recent hacking incident. The following are the numbers: the phone call was made from 410-573-9553, and the number they left for me to call is 877-573-1141."
1/17/2012	ZAP0003387	[Customer email]. "Of course I read the email properly and of course I immediately took appropriate action when I was notified of the fraudulent charges. There is absolutely no other way for someone to get this information other than from your site. I am well informed and educated on how this all works. I understand that you say the CC info was and remains secure, however, that is not true. Please have someone call me asap!!!!!!! This is INSANE!!!!"
1/17/2012	ZAP000388-89	[Customer email]. "I don't think you understand. I have unauthorized charges to my CC number that I used for my last order at Zappos. I know they are related to the site hacking, as Zappos is the only place I am listed as my maiden name. I have since changed my name and the charges were made using this billing name which I never use anymore. I am not comfortable discussing this any further through email. Could I get a real person to call me and attend to this matter? I don't appreciate the generic messages sent to me that are identical to what is

		posted all over your facebook page. I took the time to email you personally, so do the same for me.”
1/19/2012	ZAP0003514	[Customer email]. “At no point did I ask about your phones being turned off or my password. I am speaking of the missing money from my bank account, however you are falsely informing people that this is not possible and only the last 4 digits were accessed. Someone needs to contact me soon (preferably a manager) or I will be contacting my lawyer!!”
1/25/2012	ZAP0003461	Customer “claims that a new credit card and cell phone was created shortly after the Zappos security breach and she feels that it is our responsibility to pay for her credit monitoring service. I apologized to her and reiterated that her CC info was not accessed. She was not happy with this and says that she will reach out to the media and that we have lost a customer.”
1/27/2012	ZAP0003466	Customer “called in today to let us know that his Amazon account has been fraudulently used and he believes that it is stemming from our recent hack. I advised him that the passwords were cryptographically scrambled and the database that contained the critical credit card information was not accessed. I also told him that we do have an investigation with the FBI taking place right now. He requested that I forward this information and I advised him I would put it in the hands of the correct person and if they had any further questions he asked that we email him”
1/28/2012	ZAP0003481	Customer’s “wife, called upset because her CC was used to purchase in the amount of \$1000 to a different company, not Zappos, and we are the only company that she uses her CC to buy online; Bank provided information of transaction but she does not remember; Tried to advised that we wouldn’t be able to assist with the fraud transaction unless it was done on Zappos.com but [she] insisted it is because of us that the CC was used.”
1/29/2012	ZAP0003467	Customer “claiming fraud charges on her CC due to our security breach & won’t be shopping with us again, moved to OV que.”
1/29/2012	ZAP0003468	Customer “is claiming both her & husband CC was used fraudulently since our CC breach & she thinks we are the source, moved to OV que.”
1/30/2012	ZAP0003472	Customer “called as she had some fraudulent charges on her cc and her bank told her it was due to the security breach at Zappos. She wanted to know if we were going to be issuing any compensation and I advised her we were not.”
1/30/2012	ZAP0003472	Customer “said Citibank told her that her credit card fraud was

		due to Zappos breach."
2/6/2012	ZAP0003479	Customer "called in regards to the security breach. Stating that he's had his CC with Discover since 1996 and how it's linked to multiple accounts and he wanted to be compensated. I advised that unfortunately we aren't able to compensate him. I advised that the information that store the credit card information was not accessed I advised what was accessed such as name, address, phone number and the last 4 of CC. Stated he has 3 unauthorized charges after shopping on our site. I kept reiterating information. I advised I will send him an email of the compensation and Tony's [Hsieh] blog with his email address."
2/13/2012	ZAP0003483	Customer "called to let us know that she has found two more charges on her CC which are order #'s [REDACTED] and [REDACTED] Adv to file dispute. She wants it noted that she is very dissatisfied and will never shop with Zappos again."
3/4/2012	ZAP0003485	Customer "called from ___ to confirm fraud. Advised that they file a dispute for the charge. She's already cancelled her card. She advised that due to the recent breach, Discover issued her a new card. She wanted to know if this order was due to the breach. Advised that is was only bill/ship addresses and the last 4 of the cards [that were obtained by the hackers]."
3/7/2012	ZAP0003485	"Received Fraud Chargeback --- Zappos Incurred Loss of \$194.99 Due To This Being A Fraudulent Transaction --- Discover CB Case 6824401748 --- Authorizing Discover To Proceed With The Chargeback." [This is a note to the file made by a Zappos customer service representative.]
4/5/2012	ZAP0003482	Paymentech Chargeback - Fraudulent transaction totaling \$168.99.
4/5/2012	ZAP0003482	Paymentech Chargeback - Fraudulent transaction totaling \$173.00.
4/5/2012	ZAP0003482	Paymentech Chargeback - Fraudulent transaction totaling \$181.00.
4/5/2012	ZAP0003483	Paymentech Chargeback - Fraudulent transaction totaling \$184.95.
4/5/2012	ZAP0003483	Paymentech Chargeback - Fraudulent transaction totaling \$197.98.
Redacted	ZAP0003349	[Customer email]. "Mr. Hsieh – I have no idea which password I used to secure my Zappos account, so because you cut corners on security, I'll have to change every account password I have, totaling in the hundreds. When you say that you surrendered my "cryptographically scrambled password (but not your actual password), "I'm assuming you think I'm stupid enough to take comfort from you omission that anyone that could have hacked you would certainly have access to the right kind of software to unscramble the information. Further, it is cowardly to refuse phone calls during this crisis. Nonetheless, my lawyer (and

		<p>wife) assures me that the assumption is that if someone insists on utilizing email as the source of communication, there is a reasonable expectation that the recipient has received the correspondence unless a message is received bouncing it back from the recipient's server. Further, when such demands in limiting methods of communication are introduced, the onus to correct all mistakes or misconceptions in an email is placed on each recipient. Thus, if I do not hear back from you, I shall assume you concur with all the contentions contained herein. That said, should I suffer any damages as a result of your security breaches, I assume you shall incur the costs of fixing them and making me whole, damages to include covering my time.</p> <p>Since I promised a question in the subject line, I guess I should ask one. How long do you think it will take you to learn how to jump up your own [REDACTED]? I wish upon some of your loved ones the same level of pain that you have assuredly unleashed upon many of the hapless 24 million victims your penny-pinching security measures have created. I hear colo-rectal cancer is pretty bad, and karma is a bitch."</p>
Redacted	ZAP0003352	<p>[Customer email]. "I do not appreciate the way I was treated by your specialists the other day. I also believe as a previously satisfied customer of ZAPPOS.com I had every right to send the email I did to complain about said incident.</p> <p>To follow up on such a complaint with a threat that my privacy and secure information has been leaked by your company in so many words is deplorable. I didn't think an employee of yours could sink so low and then you top it off with this. I believe this is your way of leaking my information to every Tom, Dick, & Harry so to speak. (Or your disgruntled employees).</p> <p>Please be on notice I have forwarded copies of all conversations to my attorney. My personal information is to be protected at all costs since my abduction and rape. Should any harm come to me or my family I will hold your company personally liable.</p>

III. The Zappos Data Breach Inflicted Economic Damages and Other Actual Injury and Harm on Plaintiffs and Class Members.

68. Identity theft occurs when a person's PII is used without his or her permission to commit fraud or other crimes. *See* FEDERAL TRADE COMMISSION, FIGHTING BACK AGAINST

IDENTITY THEFT (Oct. 2011), www.ftc.gov/bcp/edu/microsites/ idtheft/consumers/ about-identity-theft.html.

69. According to the Federal Trade Commission (“FTC”), “the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data.” *See* FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>. Furthermore, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.” FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT 35-38 (Dec. 2010), <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>; COMMENT OF CENTER FOR DEMOCRACY & TECHNOLOGY, No. 00469, at 3; COMMENT OF STATZ, INC., No. 00377, at 11-12.

70. The FTC estimates that as many as nine million Americans are victims of identity theft and identity fraud each year. *Id.*

71. “Phishing” is a form of online identity theft that lures consumers into divulging their personal financial information to fraudulent websites, also known as spoofed websites. For example, a phisher sends an email message to an unsuspecting victim instructing him or her to click on the link to a bank’s website (provided in the email) to confirm the consumer’s account information. Unbeknownst to the consumer, the website is a convincing fake or copy of the authentic website. The unsuspecting consumer takes the bait and provides the information, thereby enabling the phisher to steal the consumer’s personal financial information. The phisher

can then use the stolen information to clean out the victim's bank accounts or commit other forms of identity theft.



73. "Pharming" is similar to phishing, albeit more sophisticated. Pharmers also send emails. A consumer compromises his or her personal financial information simply by opening a pharmer's email. The pharming email contains a virus (or Trojan horse) that installs a small software program on a consumer's computer. When the consumer attempts to visit an official website, the pharmer's software program redirects the browser to the pharmer's fake version of the website. In this way, the pharmer is able to capture the PII the consumer enters into the counterfeit website, thereby compromising the consumer's account. This also happened here.

74. As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII, the fraudsters and their customers now have Plaintiffs' and Class Members' PII. They also know that Plaintiffs and Class Members are accustomed to receiving emails from Zappos. This, in turn, makes Plaintiffs and Class Members substantially more likely

to respond to requests from Zappos for more sensitive PII, such as financial account numbers and login information, payment card information, and Social Security numbers. As such, Plaintiffs and Class Members are more likely to unknowingly give away their sensitive PII to “phishing” and “pharming” thieves who specialize in constructing spoof websites and emails mirroring Zappos.com and other popular online retailers and financial institutions.

75. According to the FTC, “Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.”

76. The United States Government Accountability Office noted in a June 2007 report on data breaches (“GAO Report”) that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person’s name. *See G.A.O., PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN* (June 2007), <http://www.gao.gov/new.items/d07737.pdf>. This type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim’s credit rating. *Id.* Victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name.” *Id.*

77. A person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once

stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

Id.

78. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money and patience to resolve. *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.⁴

79. That said, identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (e.g., obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits, or filing fraudulent tax returns using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and obtain medical services in a victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

80. PII also is a valuable commodity to identity thieves. In fact, PII is so valuable that once the information has been compromised, criminals often trade it on the "cyber black-market"

⁴ The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

for years. *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009).

81. Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other PII directly on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen PII. Strikingly, none of these websites was blocked by Google’s safeguard filtering mechanism—the “Safe Browsing list.” The study concluded:

It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it’s very “in your face.”

See [*http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/*](http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/).

82. At a FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information:

The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it’s something on the order of the life blood, the free flow of information.

Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, [*http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm*](http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm). Commissioner Swindle’s remarks are even more powerful today as consumers’ personal data functions as a “new form of currency” supporting a \$26 billion per year online advertising industry in the United States. *See* Julia Angwin and Emily Steel, *Web’s Hot New Commodity*:

Privacy, THE WALL STREET JOURNAL, available at <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>.

83. The FTC has formally recognized consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.

Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf>.

84. Recognizing the high value consumers place on their PII, many companies now offer consumers an opportunity to sell their PIII to advertisers and other third parties. The idea is to give consumers more power and control over sharing their information, including who ultimately receives it. And, by making the transaction transparent, consumers—not data thieves—will make the profits. *See, e.g., Steve Lohr, You Want My Personal Data? Reward Me for It, THE NEW YORK TIMES,* <http://www.nytimes.com/2010/07/18/business/18unboxed.html>. This business has created a new robust market for the sale and purchase of this valuable consumer data. *See Web's Hot New Commodity: Privacy,* <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>.

85. Consumers also place a high value on the *privacy* of their PII. Indeed, studies confirm that “[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US\$30.49–44.62.” *See Il-Horn Hann et al., The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2002),

<http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (emphasis added); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) INFORMATION SYSTEMS RESEARCH 254, 254 (June 2011).

86. When consumers were surveyed regarding how much they value their PII in terms of its protection against improper access and unauthorized secondary use—the very concerns at issue here—they valued the restriction of improper access to their data at between \$11.33 and \$16.58 per website, and prohibiting secondary use to between \$7.98 and \$11.68 per website. *Id.*

87. The value of Plaintiffs' and Class Members' PII on the cyber-black market is substantial. See, e.g. *The Cyber Black Market: What's Your Bank Login Worth?* (March 2011), <http://www.ribbit.net/frogstalk/id/50/the-cyber-black-market-whats-your-bank-login-worth>; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, HOW MUCH DO YOU COST ON THE BLACK MARKET?, http://www.ncix.gov/issues/cyber/identity_theft.php.

88. Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) economic damages, and other actual injury and harm, in the form of (i) actual identity theft or identity fraud, (ii) the untimely and/or inadequate notification of the Data Breach, (iii) unauthorized disclosure of their PII, (iv) loss of customer service access that was part of the services provided for by Zappos, including closure of Zappos' customer service telephone lines, which Zappos willfully severed at a time of high need by its customers, (v) loss of the unencumbered use of their extant passwords and the loss of their passwords, (vi) the oppressive Zappos.com website arbitration clause and Zappos' attempted enforcement of same, (vii) invasion of privacy, (viii) breach of the confidentiality of their PII, (ix) out-of-pocket expenses incurred to mitigate the increased risk of

identity theft and/or identity fraud pressed upon them by the Data Breach, (x) the value of their time spent mitigating the impact of the Data Breach and mitigating increased risk of identity theft and/or identity fraud including, *inter alia*, changing their Zappos.com account passwords and passwords for other accounts using the same passwords, (xi) deprivation of the value of their PII, for which there is a well-established national and international market, (xii) receipt of a diminished value of the services they paid Zappos to provide (e.g., protection of their PII), (xiii) the impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm, and (xiv) damages incurred by Zappos' violation of the contractual agreement to settle this case—for which they are entitled to compensation.

89. Although Zappos readily admits the Data Breach occurred, readily admits that Plaintiffs' and Class Members' PII was disclosed to unauthorized third parties and compromised, and strongly recommended in its January 16, 2012 emails that they reset their Zappos.com account passwords and change the passwords "on any other web site where [they] use the same or a similar password," Zappos has not offered Plaintiffs and Class Members any compensation or basic protection from the past, present, and future identity theft, identity fraud, economic damages, and other injury and harm resulting from the Data Breach. This case has resulted.

CLASS ACTION ALLEGATIONS

90. Pursuant to FED. R. CIV. P. 23, Plaintiffs bring this action against Zappos as a national class action on behalf of themselves and all members of the following class of similarly situated persons (the "Nationwide Class"):

All persons whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012. Excluded from the Nationwide Class are Defendant, any parent corporation, subsidiary

corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

91. Pursuant to FED. R. CIV. P. 23, the noted Plaintiffs also bring this action against Zappos on behalf of themselves and all members of the following classes of similarly situated persons (collectively, the "State Sub-Classes"):

ALABAMA (Elliott, Brown, and Seal): All persons in Alabama whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "Alabama Sub-Class"). Excluded from the Alabama Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

CALIFORNIA (Relethford, Ree, and Nobles): All persons in California whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "California Sub-Class"). Excluded from the California Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

FLORIDA (Penson, Braxton, and Hasner): All persons in Florida whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "Florida Sub-Class"). Excluded from the Florida Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

MASSACHUSETTS (Habashy): All persons in Massachusetts whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "Massachusetts Sub-Class"). Excluded from the Massachusetts Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

MICHIGAN (Wadsworth): All persons in Michigan whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "Michigan Sub-Class"). Excluded from the

Michigan Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

NEW YORK (Preira and O'Brien): All persons in New York whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "New York Sub-Class"). Excluded from the New York Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

TEXAS (Stevens): All persons in Texas whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012 (the "Texas Sub-Class"). Excluded from the Texas Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

92. Pursuant to FED. R. CIV. P. 23, Plaintiffs Relethford, Ree, Nobles, and Wadsworth also bring this action against Zappos on behalf of themselves and all members of the following class of similarly situated persons in the States of Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, South Carolina, Tennessee, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia (the "State Data Breach Notification Statute Sub-Class"):

All persons in Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, South Carolina, Tennessee, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia whose personally identifiable information (PII) was obtained by hackers from Zappos.com, without authorization, and compromised during the Data Breach first announced by Zappos.com on January 16, 2012. Excluded from the State Data Breach Notification Statute Sub-Class are Defendant, any parent corporation, subsidiary corporation and/or affiliate entity of Defendant, Defendant's officers, directors, employees, agents and legal representatives, and the Court.

93. The members of the Nationwide Class, State Sub-Classes, and State Data Breach Notification Statute Sub-Class are so numerous that their joinder is impracticable. According to Zappos, there are over 24 million Members of the Nationwide Class, State Sub-Classes, and State Data Breach Notification Statute Sub-Class. Their identities, physical addresses, and email addresses can be easily derived from Zappos' internal records that were used to send the January 16, 2012 emails regarding the Data Breach to Plaintiffs and Class Members.

94. The rights of each Plaintiff, each Nationwide Class Member, each respective State Sub-Class Member, and each State Data Breach Notification Statute Sub-Class Member were violated in precisely the same manner by Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII.

95. There are questions of law and fact common to the Nationwide Class, individual State Sub-Classes, and State Data Breach Notification Statute Sub-Class as a whole. The common questions of law and fact predominate over any questions affecting only individual Members of the Nationwide Class, individual State Sub-Classes, and State Data Breach Notification Statute Sub-Class⁵, and include, without limitation:

- a. whether Zappos properly designed, adopted, implemented, controlled, directed, oversaw, managed, monitored, and audited the appropriate data security processes, controls, policies, procedures, and/or protocols to safeguard and protect Plaintiffs' and Class Members' PII released and disclosed, without authorization, in the Data Breach;
- b. whether Zappos' failure to properly safeguard and protect Plaintiffs' and Class Members' PII was willful, reckless, arbitrary, capricious, and/or otherwise not in accordance with the applicable protocols, procedures, guidelines, laws, and regulations;

⁵ Unless otherwise noted, throughout the remainder of this Third Amended Consolidated Class Action Complaint, the Members of the Nationwide Class, individual State Sub-Classes, and State Data Breach Notification Statute Sub-Class will collectively be referred to as the "Class Members."

- c. whether Zappos failed to inform Plaintiffs and Class Members of the true nature and scope of the Data Breach and the unauthorized release and disclosure of their PII in a manner and within the time period required by its own internal policies and procedures and the applicable state data breach notification statutes;
- d. whether Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII constitute negligence/negligent misrepresentation;
- e. whether Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII constitute violations of various state deceptive trade practices/consumer protection acts;
- f. whether Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII constitute breach of contract;
- g. whether Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII violated various state data breach notification statutes;
- h. whether Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII constitute unjust enrichment/assumpsit;
- i. whether Zappos breached the settlement agreement entered into by the Parties and, in the process, breached the covenant (or duty) of good faith and fair dealing;
- j. whether Plaintiffs and Class Members suffered economic damages, injury, and other harm as a direct or proximate result of Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII; and
- k. whether Plaintiffs and Class Members are entitled to compensation or injunctive relief as a direct or proximate result of Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII.

96. Plaintiffs' claims are typical of the claims of the Class Members because

Plaintiffs, like all Class Members, are victims of Zappos' wrongful actions, inaction, and

omissions that caused the Data Breach, caused the unauthorized release and disclosure of their PII, and caused them to suffer economic damages and other injury and harm.

97. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, other Class Members' interests. Plaintiffs' counsel are highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

98. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been irreparably harmed as a result of Zappos' wrongful actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Litigating this case as a class action is appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the courts and Parties, (ii) it will be virtually impossible for all Class Members to intervene in this action, (iii) it will allow numerous individuals with claims too small to adjudicate on an individual basis because of prohibitive litigation costs to obtain redress for their injuries, and (iv) it will provide for court oversight of the claims process once Zappos' liability is adjudicated.

99. Certification of the Nationwide Class, the respective State Sub-Classes, and the State Data Breach Notification Statute Sub-Class, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

100. Certification of the Nationwide Class, the respective State Sub-Classes, and the State Data Breach Notification Statute Sub-Class also is appropriate under FED. R. CIV. P. 23(b)(2)

because Zappos has acted, or refused to act, on grounds generally applicable to each respective Class and Sub-Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

101. Certification of the Nationwide Class, the respective State Sub-Classes, and the State Data Breach Notification Statute Sub-Class also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Zappos. For example, one court might decide the challenged actions, inaction, and omissions are illegal and enjoin Zappos, while another court might decide the same actions, inaction, and omissions are not illegal. Individual actions also could be dispositive of the interests of the other Class Members who are not parties to such actions, and substantially impair or impede their ability to protect their interests.

102. Zappos' wrongful actions, inaction, and omissions are generally applicable to the Nationwide Class and the Sub-Classes as a whole and, therefore, Plaintiffs also seek equitable remedies for the Nationwide Class and Sub-Classes.

103. Zappos' systemic policies and practices also make injunctive relief for the Nationwide Class and Sub-Classes appropriate.

104. Absent a class action, Zappos will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class Members.

CLAIMS AND CAUSES OF ACTION

COUNT I

NEGLIGENCE/NEGLIGENT MISREPRESENTATION

(For the Nationwide Class under Nevada Common Law and State Sub-Classes under the Respective States' Common Law)

105. The preceding factual statements and allegations are incorporated by reference.

106. Zappos had (and continues to have) a duty to Plaintiffs and Class Members to safeguard and protect their PII according to, *inter alia*, the representations and promises on its website and in its “Safe Shopping Guarantee.”

107. Zappos had (and continues to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage of private, non-public PII within its possession, custody and control) and the affirmative duty expressly imposed on Zappos from its representations to safeguard and protect Plaintiffs' and Class Members' PII.

108. Zappos had (and continues to have) a duty to design, adopt, implement, control, direct, oversee, manage, monitor and/or audit appropriate data security processes, controls, policies, procedures and/or protocols in order to safeguard and protect the PII entrusted to it—including Plaintiffs' and Class Members' PII.

109. The representations, standards, and duties outlined above are for the express purpose of protecting Plaintiffs' and Class Members' PII.

110. Zappos' above-referenced representations, standards, and duties were made in the ordinary course of its regular business with the intent to induce Plaintiffs and Class Members to use its website and provide their PII to Zappos for the purpose of purchasing shoes, apparel, and other merchandise from Zappos.

111. Zappos knew that reasonable consumers—such as Plaintiffs and Class Members—would rely on the above-referenced representations, standards, and duties on its website and provide their PII to Zappos for the purpose of purchasing shoes, apparel, and other merchandise from Zappos.

112. Zappos violated these representations, standards, and duties by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and Class Members' PII, as Zappos promised to do.

113. It was reasonably foreseeable—in that Zappos knew or should have known—that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

114. Zappos, by and through its above negligent actions, inaction, and omissions unlawfully breached its responsibilities and duties to Plaintiffs and Class Members by, among other things, failing to safeguard and protect their PII within its possession, custody and control and, in fact, wrongfully releasing and disclosing it to unauthorized third parties through Zappos' unprotected servers.

115. Zappos, by and through its above negligent actions and/or inaction, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within its possession, custody, and control.

116. The release and disclosure of Plaintiffs' and Class Members' PII to third parties was without Plaintiffs' and Class Members' authorization or consent.

117. But for Zappos' negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Class Members, their PII would not have been disseminated to the world and compromised for no lawful purpose.

118. Plaintiffs' and Class Members' PII was wrongfully released, disclosed, transferred, sold, opened, read, mined, compromised, and otherwise used without their authorization as a direct and proximate result of Zappos' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within its possession, custody, and control.

119. Plaintiffs and Class Members justifiably relied on Zappos' website representations to safeguard and protect their PII, which Zappos failed to do, as evidenced by the Data Breach and its substantial negative impact on Plaintiffs and Class Members.

120. As a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation. Zappos' Zappos' wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence/negligent misrepresentation.

COUNT II

**VIOLATION OF STATE DECEPTIVE TRADE PRACTICES
AND CONSUMER PROTECTION ACTS**

(For the Nationwide Class Under Nevada Law and State Sub-Classes under the Respective States' Statutes)

121. The preceding factual statements and allegations are incorporated by reference.

122. Pursuant to MASS. GEN. LAWS ch. 93A, § 9 Habashy sent Zappos a demand letter on January 24, 2012.

123. The uniform publication and advertising of Zappos' commitment to preserving and maintaining the confidentiality and integrity of PII entrusted to it in connection with sales of shoes, apparel, and other merchandise to its customers—including Plaintiffs' and Class Members' PII—were consumer transactions as defined by the deceptive trade practices and consumer protection acts set forth below.

124. Zappos is a supplier as defined by the deceptive trade practices and consumer protection acts set forth below. Zappos is engaged in, and its acts and omissions affect, trade and commerce. Zappos' above-described wrongful actions, inaction, and omissions were committed in the course of Zappos' business of marketing, offering for sale, and selling merchandise and data security services, which Plaintiffs and Class Members purchased, throughout the United States, including in Nevada.

125. Plaintiffs and Class Members are persons and consumers as defined by the deceptive trade practices and consumer protection acts set forth below.

126. Zappos' retail sales of shoes, apparel, and other merchandise to Plaintiffs and Class Members were (and continue to be) the operations of consumer oriented enterprise having a broad impact on consumers at large as defined by the deceptive trade practices and consumer protection acts set forth below.

127. Zappos' uniform publication and advertising of its commitment to safeguard and protect the confidentiality and integrity of PII entrusted to it in connection such retail consumer sales transactions—including Plaintiffs' and Class Members' PII—that, in fact, Zappos failed to do (as evidenced by the Data Breach)—constitute deceptive acts and practices as defined by the deceptive trade practices and consumer protection acts set forth below.

128. Zappos violated the deceptive trade practices and consumer protection acts set forth below—which directly and proximately caused the Data Breach—by engaging in unfair, unlawful, unconscionable, and/or deceptive acts and practices, all of which offend public policies and are immoral, unethical, unscrupulous, and/or substantially injurious to consumers, including Plaintiffs and Class Members; to wit, *inter alia*:

- a. uniformly misrepresenting to Plaintiffs and Class Members that their PII would be preserved in strictest confidence with the utmost data integrity, safeguarded, and protected when, in fact, Zappos routinely failed to do so;
- b. uniformly failing to disclose to Plaintiffs and Class Members the material fact that their PII, in fact, was not properly safeguarded and protected;
- c. uniformly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and industry standards for safeguarding and protecting Plaintiffs' and Class Members' PII within its possession, custody, and control;
- d. uniformly failing to properly encrypt Plaintiffs' and Class Members' PII;
- e. uniformly failing to properly train its employees in principles of cyber-security policies and procedures including, *inter alia*, handling, storing, safeguarding, and protecting PII;
- f. uniformly failing to adequately inform Plaintiffs and Class Members about the nature and scope of the Data Breach, and the true risk of the potential identity theft and identity fraud resulting from the Data Breach; and
- g. uniformly misrepresenting the true nature and scope of the Data Breach in post-Data Breach oral and written communications with Class Members.

129. Zappos' conduct, as set forth above, would likely deceive a reasonable consumer. Plaintiffs and Class Members relied on such material misrepresentations to their detriment. They, in fact, were deceived.

130. Zappos' above-described wrongful actions, inaction, and omissions also constitute (and continue to constitute) unconscionable conduct as defined by the deceptive trade practices and consumer protection acts set forth below.

131. As a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation. The economic damages, injury, and harm suffered by Plaintiffs and Class Members sufficiently outweigh any possible justifications or motives for Zappos' failure to safeguard and protect their PII.

132. Zappos wrongfully released and disclosed Plaintiffs' and Class Members' PII without authorization and for no lawful purpose. Unless restrained and enjoined, Zappos will continue to engage in the above-described wrongful conduct.

133. Due to Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, Plaintiffs, on behalf of themselves and the Nationwide Class, assert claims against Zappos for violating the Nevada Deceptive Trade Practices Act, NEV. REV. STAT. § 598.0903, *et seq.* by, *inter alia*:

- a. knowingly making a false representation as to the characteristics, uses, and benefits of its services (NEV. REV. STAT. § 598.0915(5));

- b. knowingly making other false representations in connection with online retail transactions (NEV. REV. STAT. § 598.0915(15)); and
- c. failing to disclose material facts in connection with the online retail sale of goods (NEV. REV. STAT. § 598.0923(2)).

134. By engaging in the above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, Zappos violated the state deceptive trade practices and consumer protection acts set forth below prohibiting (i) representations "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," (ii) representations that "goods and services are of a particular standard, quality or grade, if they are of another," and (iii) "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Zappos' continued acceptance of Plaintiffs' and Class Members' credit card and debit card payments for merchandise purchases after Zappos (i) knew, or should have known, of the Data Breach or computer system problems giving rise to the Data Breach, and (ii) before it corrected the computer system problems giving rise to the Data Breach constitute unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices in violation of the state deceptive trade practices and consumer protection acts set forth below.

135. Accordingly, Plaintiffs, on behalf of themselves and their respective State Sub-Classes, also assert claims against Zappos for violating the following deceptive trade practices and consumer protection acts:

- a. Florida Deceptive and Unfair Trade Practices Act, FLA. STAT. ANN. § 501.204(1), *et seq.*;
- b. Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e), (s) and (cc), *et seq.*;

- c. New York Business Law, N.Y. GEN. BUS. LAW §§ 349(a); 598.0915(5) and (7), *et seq.*; and
- d. Texas Deceptive Trade Practices/Consumer Protection Act, TEX. BUS. & COM. CODE § 17.46(a), (b)(5) and (7) and § 17.50(a)(3), *et seq.*

136. Plaintiffs bring this action for the relief requested and for the public benefit in order to promote the public interests in the provision of truthful, non-deceptive information to allow consumers to make informed purchasing decisions, and protect Plaintiffs and Class Members and the public from Zappos' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful acts practices. Zappos' wrongful actions, inaction, and omissions have had widespread impact on the public at large, inflicting economic damages, and other injury and harm, on over 24 million persons across the United States.

COUNT III

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

(CAL. BUS. & PROF. CODE §17200, *et seq.*)
(For the California Sub-Class)

137. The preceding factual statements and allegations are incorporated by reference.

138. The California Unfair Competition Law, CAL. BUS. & PROF. CODE §17200, *et seq.* (“UCL”), prohibits any “unlawful,” “fraudulent,” or “unfair” business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law. By reason of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, Zappos engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

139. Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members have suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions

including, *inter alia*, the unauthorized release and disclosure of their PII—for which they are entitled to (i) compensation for Zappos' violations of the Security Requirements for Consumer Records Act, CAL. CIV. CODE §§ 1798.29 and 1798.80, *et seq.*, and (ii) the expense to protect against the use, and mitigate the loss, of the unlawful and unauthorized use of their PII.

140. In the course of conducting business, Zappos committed “unlawful” business practices by, *inter alia*, failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and industry standards for safeguarding and protecting Plaintiffs’ and Class Members’ PII within its possession, custody, and control, thereby violating the Security Requirements for Consumer Records Act, CAL. CIV. CODE §§ 1714, 1798.29 and 1798.80, *et seq.* Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members reserve the right to allege other violations constituting other unlawful business acts or practices.

141. Zappos also violated the UCL by failing to timely and completely notify Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members about the true nature and scope of the Data Breach and their wrongfully released and disclosed PII. If Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members had been properly notified, they could have (and would have) taken appropriate precautions to safeguard and protect their PII.

142. Zappos’ above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs’ and Class Members’ PII also constitute “unfair” business acts and practices within the meaning of CAL. BUS. & PROF. CODE § 17200, *et seq.*, in that Zappos’ conduct was (and continues to be) substantially injurious to consumers, offensive to public policy, immoral, unethical, oppressive, and unscrupulous; the

gravity of Zappos' conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Zappos' legitimate business interests other than its above-described wrongful actions, inaction, and omissions.

143. California Business and Professions Code § 17200 also prohibits any "fraudulent business act or practice." Zappos' claims, nondisclosures and misleading statements, as set forth above, were false, misleading, and likely to deceive the consuming public within the meaning of CAL. BUS. & PROF. CODE § 17200.

144. Zappos' above-described wrongful actions, inaction, and omissions caused (and continue to cause) substantial injury to Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members. Zappos wrongfully released and disclosed their PII. Unless restrained and enjoined, Zappos will continue to engage in the above-described wrongful conduct leading to further unauthorized disclosures of its customers' PII.

145. As a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs Relethford's, Ree's, and Nobles' and the California Sub-Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation. The economic damages, injury, and harm suffered by Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members sufficiently outweigh any possible justifications or motives for Zappos' failure to safeguard and protect their PII.

COUNT IV

VIOLATION OF SECURITY REQUIREMENTS FOR CONSUMER RECORDS

(CAL. CIV. CODE §1798.29 and 1798.80, *et seq.*)

(For the California Sub-Class)

146. The preceding factual statements and allegations are incorporated by reference.

147. California law requires any business obtaining PII from its customers (including the PII at issue here) to implement and maintain reasonable data security procedures and practices to protect such information from unauthorized access, destruction, use, modification, or disclosure.

148. CAL. CIV. CODE §§ 1798.29 and 1798.82 further require any business retaining PII obtained from its customers to promptly and “in the most expedient time possible and without unreasonable delay” disclose any breach of the security of the system containing such retained data.

149. Zappos failed to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiffs Relethford’s, Ree’s, and Nobles’ and the California Sub-Class Members’ PII that, in turn, directly and proximately caused the Data Breach and the unauthorized disclosure of their PII.

150. Zappos also unreasonably delayed and failed to disclose the true nature and scope of the Data Breach to Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members in the most expedient time possible and without unreasonable delay when it knew, or reasonably believed, the Data Breach had occurred and their PII had been wrongfully released and disclosed. In fact, Zappos has gone out of its way to do the opposite.

151. On information and belief, no law enforcement agency has informed Zappos that notifying Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members about the true nature and extent of the Data Breach would impede any investigation, nor did any law enforcement agency direct Zappos not to make such notification.

152. Zappos also failed to comply with the privacy notification rights required by CAL. CIV. CODE § 1798.83.

153. As a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs Relethford's, Ree's, and Nobles' and the California Sub-Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation.

COUNT V

VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT

**(CAL. CIV. CODE §1750, *et seq.*)
(For the California Sub-Class)**

154. The preceding factual statements and allegations are incorporated by reference.

155. Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members are “consumers” within the meaning of CAL. CIV. CODE § 1761(d), as they purchased shoes, apparel, merchandise, and data security services from Zappos for personal, family and/or household purposes, and not for resale.

156. The shoes, apparel and other merchandise are “goods” within the meaning of CAL. CIV. CODE § 1761(a), as they are tangible chattels bought for private purposes.

157. The purchases of shoes, apparel, other merchandise, and data security services from Zappos by Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members were (and continue to be) “transactions” within the meaning of CAL. CIV. CODE § 1761(e).

158. Zappos’ above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs Relethford’s, Ree’s, and Nobles’ and the California Sub-Class Members’ PII constitute deceptive acts and practices, unlawful methods of competition, and unfair acts, as defined by CAL. CIV. CODE § 1750, *et seq.*, to their detriment.

159. Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members reasonably expected that Zappos would safeguard and protect their PII. Based on this reasonable expectation, they purchased shoes, apparel, other merchandise, and data security services from Zappos. Despite its website promises, Zappos failed to safeguard and protect their PII in violation of the following California Consumer Legal Remedies Act provisions: (i) CAL. CIV. CODE § 1770(a)(5) (representing goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities which they do not have), (ii) CAL. CIV. CODE § 1770(a)(7) (representing goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another), and (iii) CAL. CIV. CODE § 1770(a)(14) (representing a transaction confers or involves rights, remedies or obligations which it does not have or involve, or which are prohibited). Zappos also failed to inform Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members that it had failed to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security and confidentiality of their PII.

160. As a direct and proximate result of Zappos' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs Relethford's, Ree's, and Nobles' and the California Sub-Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation.

161. Pursuant to CAL. CIV. CODE § 1780(a), therefore, Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members seek (i) actual damages, (ii) an order enjoining Zappos from engaging in the wrongful methods, acts and/or practices alleged herein, (iii) restitution, (iv) punitive damages, and (v) all other affirmative relief this Court deems just and proper. Plaintiffs Relethford, Ree, and Nobles and the California Sub-Class Members also seek to recover their attorneys' fees, litigation expenses, and court costs.

COUNT VI

BREACH OF CONTRACT **(For the Nationwide Class Under Nevada Law)**

162. The preceding factual statements and allegations are incorporated by reference.

163. Plaintiffs and Class Members purchased shoes, apparel, and other merchandise from Zappos in exchange for money transferred to Zappos via Zappos' website, thereby creating a contract between the Parties.

164. As a uniform condition precedent to the completion of such purchase and sale transactions, including those involving Plaintiffs and Class Members, Zappos required them to provide Zappos with their PII, which provides measurable benefits to Zappos in that Plaintiffs' and Class Members' PII allows Zappos to obtain knowledge about and analyze their shopping habits that, in turn, empowers Zappos to target market carefully selected shoes, apparel, and other merchandise directly and uniquely to each of its past and present online customers

(including Plaintiffs and Class members). Zappos' target marketing approach makes its website more user friendly which, in turn, encourages and facilitates more actual sales at a greater dollar value per sale, thereby increasing Zappos' revenue and profits.

165. Plaintiffs' and Class Members' PII also has intrinsic value on the robust domestic and international "big data" market. On information and belief, Zappos realizes additional value from Plaintiffs' and Class Members' PII via other data mining techniques known only by Zappos at this time that will be revealed in the discovery process.

166. Through the statements and representations regarding its data security measures on its website, and its own password requirements, Zappos explicitly and impliedly promised Plaintiffs and the Class Members that it would safeguard and protect their PII.

167. Indeed, Zappos' covenant that it would safeguard and protect their PII is a material term of its contracts with Plaintiffs and Class Members. Zappos represented and promised Plaintiffs and Class Members that "Zappos.com servers are protected by secure firewalls—communication management computers specially designed to keep information secure and inaccessible by other Internet users. So you're absolutely safe while you shop."

168. Plaintiffs and Class Members relied on this covenant and, in fact, would not have disclosed their PII to Zappos without assurances that their PII would be properly safeguarded. In the alternative, and to the extent Zappos' covenant to safeguard and protect Plaintiffs' and Class Members' PII is not an express term of the Parties' purchase and sale contracts, it is an implied term in such contracts.

169. Plaintiffs and Class Members fulfilled all of their obligations under their purchase and sale contracts with Zappos by providing their funds and PII to Zappos in exchange for shoes, apparel, and other merchandise.

170. Zappos, on the other hand, did not live up to all of its obligations under its purchase and sale contracts with Plaintiffs and Class Members by failing to safeguard and protect their PII, which directly or caused caused Plaintiffs and Class Members to suffer economic damages and other actual injury and harm.

171. Zappos' above-described wrongful conduct constitutes breach of contract under Nevada common law.

COUNT VII

BREACH OF STATE DATA BREACH NOTIFICATION STATUTES (For the State Data Breach Notification Statute Sub-Class)

172. The preceding factual statements and allegations are incorporated by reference.

173. Legislatures in the states listed below have enacted data breach notification statutes, which generally require all persons and businesses conducting business within such states that own or license computerized data containing PII to timely and completely disclose to all residents of the state any data breach of such computerized data by which their PII was acquired by an unauthorized person. These statutes require the disclosure of data breaches to be made expediently and without unreasonable delay.

174. The Data Breach was a breach of Zappos' computer system within the meaning of the below-listed state data breach notification statutes, which covered and protected Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members' wrongfully disclosed and compromised PII.

175. Even though Zappos has long since admitted the Data Breach occurred, to date, Zappos has failed and refused to timely, clearly, and comprehensively notify Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members about the true nature and scope of the Data Breach. In fact, Zappos has gone out

of its way to do the reverse—repeatedly misrepresenting to Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members that it was not responsible for the Data Breach, their credit card and debit card numbers were not taken, and the Data Breach was not the cause of their subsequent fraudulent charges, identity theft/identity fraud, and other post-Data Breach experiences. Zappos' above-described wrongful actions, inaction, and omissions violated (and continue to violate) the following state data breach notification statutes (as enforced through state consumer protection statutes, where applicable and as noted):

- (i) ALASKA STAT. ANN. § 45.48.010(a), *et seq.*, as enforced through ALASKA STAT. ANN. §§ 45.50.471-45.50.561;
- (ii) CAL. CIV. CODE § 1798.83(a), *et seq.*;
- (iii) COLO. REV. STAT. ANN. § 6-1-716(2), *et seq.*;
- (iv) DEL. CODE ANN. TIT. 6 § 12B-102(a), *et seq.*;
- (v) D.C. CODE § 28-3852(a), *et seq.*;
- (vi) GA. CODE ANN. § 10-1-912(a), *et seq.*;
- (vii) HAW. REV. STAT. § 487N-2(a), *et seq.*;
- (viii) ILL. COMP. STAT. ANN. 530/10(a), *et seq.*, as enforced through the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. ANN. § 505/2, *et seq.*;
- (ix) IOWA CODE ANN. § 715C.2(1), *et seq.*;
- (x) KAN. STAT. ANN. § 50-7a02(a), *et seq.*;
- (xi) KY. REV. STAT. ANN. § 365.732(2), *et seq.*;
- (xii) LA. REV. STAT. ANN. § 51:3074(A), *et seq.*;
- (xiii) MD. CODE ANN., COMMERCIAL LAW § 14-3504(b), *et seq.*, as enforced through Title 13 of the Maryland Consumer Protection Act;

- (xiv) MICH. COMP. LAWS ANN. § 445.72(1), *et seq.*;
- (xv) MONT. CODE ANN. § 30-14-1704(1), *et seq.*, as enforced through MONT. CODE ANN. § 30-14-103;
- (xvi) N.H. REV. STAT. ANN. § 359-C:20(1)(a), *et seq.*;
- (xvii) N.J. STAT. ANN. § 56:8-163(a), *et seq.*, as enforced through N.J. STAT. ANN. § 56:8-1, *et seq.*;
- (xviii) N.C. GEN. STAT. ANN. § 75-65(a), *et seq.*, as enforced through N.C. GEN. STAT. ANN. § 75-1.1;
- (xix) N.D. CENT. CODE ANN. § 51-30-02, *et seq.*, as enforced through N.D. CENT. CODE ANN. CH. 51-15;
- (xx) OR. REV. STAT. ANN. § 646A.604(1), *et seq.*;
- (xxi) S.C. CODE ANN. § 39-1-90(A), *et seq.*;
- (xxii) TENN. CODE ANN. § 47-18-2107(b), *et seq.*;
- (xxiii) VA. CODE. ANN. § 18.2-186.6(B), *et seq.*;
- (xxiv) WASH. REV. CODE ANN. § 19.255.010(1), *et seq.*;
- (xxv) WIS. STAT. ANN. § 134.98(2), *et seq.*; and
- (xxvi) WYO. STAT. ANN. § 40-12-502(a), *et seq.*

176. Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members suffered injury and harm as a direct and proximate result of Zappos' failure and refusal to provide them with timely and accurate notice of the true nature and scope of the Data Breach as required by the above-listed state data breach notification statutes. Had Zappos provided such timely and accurate notice, Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members could have (and would have) taken the appropriate measures to protect themselves from identity theft, identity fraud, and other injury and harm that, in fact, has already occurred and most likely will occur again in the future.

177. On information and belief, no law enforcement agency has informed Zappos that notifying Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members about the true nature and extent of the Data Breach would impede any investigation, nor did any law enforcement agency direct Zappos not to make such notification.

178. Plaintiffs Relethford, Ree, Nobles, and Wadsworth and the State Data Breach Notification Statute Sub-Class Members seek all remedies available under the above-listed state data breach notification statutes including, without limitation, (i) financial compensation, (ii) equitable relief, including injunctive relief and disgorgement of Defendants' gross revenues (as described above), and (iii) attorneys' fees, litigation expenses, and costs, as provided by law.

COUNT VIII

UNJUST ENRICHMENT/ASSUMPSIT

(For the Nationwide Class Under Nevada Law and State Sub-Classes Under the Respective States' Common Law)

179. The preceding factual statements and allegations are incorporated by reference.

180. As described above, Plaintiffs and Class Members conferred a valuable benefit on Zappos in the form of their PII that Zappos (and, on information and belief, Amazon.com, its parent corporation), among other things, could use to track their buying habits and target market specific shoes, apparel, and other merchandise that, in turn, increased Zappos' (and therefore Amazon.com's) revenues and profit. Plaintiffs' and Class Members' PII also has intrinsic value on the robust domestic and international "big data" market. On information and belief, Zappos realizes additional value from Plaintiffs' and Class Members' PII via other data mining techniques known only by Zappos at this time that will be revealed in the discovery process.

181. By providing their valuable PII to Zappos, Plaintiffs and Class Members conferred substantial commercial and financial advantages on Zappos and its affiliates.

182. Although Zappos appreciated (and continues to appreciate) such substantial commercial and financial advantages conferred on it by Plaintiffs and Class Members, Zappos provided no like-kind benefits to Plaintiffs and Class Members in return regarding their PII, thereby rendering the substantial commercial and financial advantages conferred on Zappos by Plaintiffs and Class Members gratuitous.

183. In light of the Data Breach and corresponding unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII, under principles of equity and good conscience, Zappos should not be rewarded for failing to safeguard and protect their PII; to wit, Zappos should not continue to be unjustly enriched by the substantial commercial and financial advantages generated by their PII while, at the same time, failing to safeguard and protect it and, in fact, openly and wantonly denying any responsibility for the Data Breach and refusing to compensate Plaintiffs and Class Members for their above-described economic damages, and other actual injury and harm.

184. Accordingly, Plaintiffs, on behalf of themselves and the Class Members, seek to impose a constructive trust over (and recover) all amounts by which Zappos has been (and continues to be) unjustly enriched. Plaintiffs and Class Members are also entitled to restitution and/or disgorgement of Zappos' ill-gotten gains pursuant to common law.

COUNT IX

BREACH OF THE COVENANT (OR DUTY) OF GOOD FAITH AND FAIR DEALING
(For the Nationwide Class Under Nevada Law)

185. The preceding factual statements and allegations are incorporated by reference.

A document page featuring 15 horizontal black redaction bars of varying lengths, distributed across the page. The bars are positioned at approximately the following vertical offsets from the top: 10, 25, 40, 55, 70, 85, 100, 115, 130, 145, 160, 175, 190, 205, 220, and 235. The page is otherwise blank with no text or other markings.

COUNT X

BREACH OF THE SETTLEMENT AGREEMENT
(For the Nationwide Class Under Nevada Law)

200. The preceding factual statements and allegations are incorporated by reference.

[REDACTED]

RELIEF REQUESTED

204. The preceding factual statements and allegations are incorporated by reference.

205. **DAMAGES.** As a direct and proximate result of Zappos' wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) economic damages, and other actual injury and harm, in the form of (i) actual identity theft or identity fraud, (ii) the untimely and/or inadequate notification of the Data Breach, (iii) unauthorized disclosure of their PII, (iv) loss of customer service access that was part of the services provided for by Zappos, including closure of Zappos' customer service telephone lines, which Zappos willfully severed at a time of high need by its customers, (v) loss of the unencumbered use of their extant passwords and the loss of their passwords, (vi) the oppressive Zappos.com website arbitration clause and Zappos' attempted enforcement of same, (vii) invasion of privacy, (viii) breach of the confidentiality of their PII, (ix) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed

upon them by the Data Breach, (x) the value of their time spent mitigating the impact of the Data Breach and mitigating increased risk of identity theft and/or identity fraud including, *inter alia*, changing their Zappos.com account passwords and passwords for other accounts using the same passwords, (xi) deprivation of the value of their PII, for which there is a well-established national and international market, (xii) receipt of a diminished value of the services they paid Zappos to provide (e.g., protection of their PII), (xiii) the impending, imminent, and ongoing increased risk of future identity theft, identity fraud, economic damages, and other actual injury and harm, and (xiv) damages incurred by Zappos' violation of the contractual agreement to settle this case—for which they are entitled to compensation. Plaintiffs and Class Members also are entitled to recover statutory damages under the applicable state statutes set forth above. Plaintiffs' and Class Members' damages were (and continue to be) foreseeable by Zappos and exceed the minimum jurisdictional limits of this Court.

206. **DOUBLE/TREBLE DAMAGES.** Plaintiffs and Class Members also are entitled to recover double or treble damages for Zappos' knowing, willful, intentional, unconscionable and deceptive acts and practices under the applicable state statutes set forth above.

207. **PUNITIVE DAMAGES.** Plaintiffs and Class Members also are entitled to punitive damages from Zappos as punishment and to deter such wrongful conduct in the future.

208. **EQUITABLE RELIEF.** Plaintiffs and Class Members also are entitled to recover all amounts by which Zappos has been unjustly enriched. Plaintiffs and Class Members are also entitled to restitution and/or disgorgement of Zappos' ill-gotten gains pursuant to common law.

209. **INJUNCTIVE RELIEF.** Plaintiffs and Class Members also are entitled to injunctive relief in the form of, *inter alia*, without limitation, (i) credit monitoring, (ii) internet monitoring, (iii) identity theft insurance (or its equivalent), and (iv) clear, detailed, and comprehensive notice

to Plaintiffs and Class Members precisely describing the nature and extent of the Data Breach (including an adequate telephone bank of customer representatives to answer any questions about the notice), so Plaintiffs and Class Members may take any additional appropriate steps to protect themselves, their identities, and their finances.

210. ATTORNEYS' FEES, LITIGATION EXPENSES AND COURT COSTS. Plaintiffs and Class Members also are entitled to recover their attorneys' fees, litigation expenses, and court costs in prosecuting this action under the applicable the state laws set forth above.

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs be designated the Nationwide Class, State Sub-Class, and State Data Breach Notification Statute Sub-Class Representatives, respectively, and (iii) Plaintiffs' Counsel be appointed as Class Counsel. Plaintiffs, on behalf of themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Zappos for:

- (i) actual, consequential, incidental and/or nominal damages (as set forth above) to be determined by the trier of fact;
- (ii) statutory damages;
- (iii) double/treble damages (as available);
- (iv) punitive damages;
- (v) all amounts by which Zappos has been unjustly enriched;
- (vi) restitution or disgorgement of Zappos' ill-gotten gains;
- (vii) appropriate injunctive relief (as set forth above);
- (viii) pre- and post-judgment interest at the highest legal rates;
- (ix) attorneys' fees and litigation expenses; and
- (x) costs of suit.

Plaintiffs, on behalf of themselves and Class Members, further request that this Court (i) compel specific performance by Zappos and enforce the material settlement terms agreed to by the Parties in the MOU, including the determination and award of Plaintiffs' Counsel's attorneys' fees, costs, and expenses, and Plaintiffs' incentive awards, and, in all things, (ii) grant such other and further relief this Court deems just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class Members, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Date: September 28, 2015.

Respectfully submitted,

By: /s/ Ben Barnow
Ben Barnow (*pro hac vice*)
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Telephone: 312.621.2000
Facsimile: 312.641.5504
Email: b.barnow@barnowlaw.com

Richard L. Coffman (*pro hac vice*)
THE COFFMAN LAW FIRM
505 Orleans St., Fifth Floor
Beaumont, TX 77701
Telephone: 409.833.7700
Facsimile: 866.835.8250
Email: rcoffman@coffmanlawfirm.com
Jeremiah Frei-Pearson (*pro hac vice*)

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
1311 Mamaroneck Avenue, Suite 220
White Plains, NY 10605
Telephone: 914.298.3281
Facsimile: 914.824.1561
Email: jfrei-pearson@fbfglaw.com

Marc L. Godino (*pro hac vice*)
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: 310.201.9150
Facsimile: 310.201.9160
Email: mgodino@glancylaw.com

PLAINTIFFS' INTERIM CO-LEAD COUNSEL

David C. O'Mara
O'MARA LAW FIRM, P.C.
311 E. Liberty St.
Reno, NV 89501
Telephone: 775.323.1321
Facsimile: 775.323.4082
Email: david@omaralaw.net

PLAINTIFFS' LIAISON COUNSEL

CERTIFICATE OF SERVICE

I hereby certify that on September 28, 2015, I electronically filed the foregoing Plaintiffs' Third Amended Consolidated Class Action Complaint with the Clerk of Court by using the CM/ECF system, thereby electronically serving a copy of same on all counsel of record.

/s/ Ben Barnow
Ben Barnow

EXHIBIT A

(FILED UNDER SEAL)